

عنوان مقاله:

معماری چند لایه در حفاظت از اطلاعات به روش قرار دادن اطلاعات Embedded رمزنگاری شده به صورت ضمنی در برنامه Bind شده

محل انتشار:

دومین همایش ملی فناوری های نوین در مهندسی برق و کامپیوتر (سال: 1393)

تعداد صفحات اصل مقاله: 6

نویسنده:

احمدعلی زارعی - دانشجوی کارشناسی مهندسی فناوری اطلاعات دانشگاه پیام نور واحد شیراز

خلاصه مقاله:

معماری چند لایه از تکنیک های ابداعی مختلف نظیر ایده های نو در رمزنگاری، رمزگذاری، استتار، پنهان سازی، کنترل ضمنی Binding برنامه های کاربردی، استفاده از فایل های Embedded شده، محیط تولید محتوا، ابزار های گرافیکی نظیر Spot و سایر تکنیک ها برای ایجاد بالاترین سطح در حفاظت از اطلاعات استفاده می کند. ما از روش استتار که یکی از مهمترین شیوه های حفاظتی می باشد ایده گرفتیم و به کمک تکنیک Binding این روش را برای داده های رایانه ای پیاده سازی کردیم در این روش ما به دنبال راهی بودیم که بتوان اطلاعات را در برنامه های کاربردی و فایل هایی که در سیستم عامل وجود دارد پنهان کنیم بدون آنکه تغییری در حجم، ظاهر، خصوصیات و عملکرد آن ها ایجاد شود که به کمک انقیاد این کار میسر شد. یعنی به جای اینکه فایل اطلاعاتی خود را به این برنامه های کاربردی در سیستم عامل اضافه کنیم در یک محیط تولید محتوا این اطلاعات حساس را به صورت توکار اضافه کرده و سپس برنامه های کاربردی مورد نظر را به آن Bind کردیم بدین ترتیب عمل انقیاد، برنامه های کاربردی را در برنامه ما فراخوانی می کرد و فایل خروجی تولید می نمود که دقیقاً مشابه با همان برنامه کاربردی (از لحاظ حجم، ظاهر، عملکرد، ...) بود. به این دلیل که عمل انقیاد فقط فراخوانی می کند و این عمل حجم ناچیزی دارد و تنها حجم فایل مربوط به اطلاعاتی می شد که به صورت توکار در برنامه قرار گرفته است. از طرفی تولید محتوا در برنامه صورت می گرفت و به همین دلیل نیاز به نوشتن آن روی حافظه دائمی و سپس حفاظت از آن نبود و مزیت بزرگی محسوب می شد زیرا قرار گرفتن اطلاعات بر روی حافظه دائمی حتی با وجود فرمت شدن هارد باز هم قابل بازیابی است در مرحله بعدی نحوه دسترسی به اطلاعات مطرح بود که در نخستین مرحله برای آماده سازی نرم افزار برای دریافت رمز به کمک ابزار گرافیکی Spot محلی از برنامه کاربردی Bind شده را در نظر می گرفتیم که با کلیک روی آن ناحیه خاص نرم افزار به صورت ضمنی آماده دریافت پسورد و کنترل آن شود و در تمام این مراحل فقط برنامه کاربردی در حال اجرا و رویت است و کلیه عملیات به صورت ضمنی انجام می شود که باعث می شد نرم افزار های قفل شکن و افراد غیر مجاز در شکستن رمز ناموفق گردند همچنین از یک الگوریتم رمزگذاری همروند استفاده می شود که با ورود هر رمز به صورت ضمنی کنترل انجام شده و در صورت اشتباه بودن آن، نرم افزار کلیه دسترسی ها را غیر فعال می نماید. در حقیقت ما به کمک تکنیک هایی که مطرح شد، فایلی مشابه یکی از برنامه های کاربردی ویندوز نظیر ماشین حساب Notepad عکس و غیره ایجاد می کنیم که از لحاظ خصوصیات، ظاهر، حجم، عملیات و غیره با فایل اصلی هیچ تفاوتی ندارد و تنها تفاوت آن وجود اطلاعات پنهان شده ما در آن فایل ها و همچنین دستوراتی نظیر رمز ها و کنترل ها برای دسترسی به آن اطلاعات می باشد و به کمک عملیات خاصی از طریق آن برنامه می توان به اطلاعات دسترسی پیدا نمود.

کلمات کلیدی:

رمزنگاری، رمزگذاری ضمنی، معماری چند لایه حفاظتی، انقیاد

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/337616>



